Appendix B: Program Maturity Assessment

Municipal open data programs create privacy risks around re-identification, data quality and equity, and public trust. FPF provides the following assessment framework in order to help municipalities around the United States better evaluate their organizational structures and data handling practices related to open data privacy.

In conducting their own assessments, we recommend municipal leaders incorporate the following into their analyses: any public statements about the municipality's open data program, privacy commitments, and use of personal data; interviews with internal and external staff who have responsibility for open data or privacy, or who contribute to or rely on the municipality's published open datasets; public discussions with local community advisors about open data and privacy values within the community; expert opinions or guidance from statistical disclosure control professionals about calculating and mitigating re-identification risks; any relevant case law or legal opinions related to the intersection of public records laws and individual privacy; and any relevant vendor contracts that might condition the sharing of personal data. These materials should support and document the municipal open data program's activities in each privacy domain, and justify its maturity measures.

Municipalities should apply a consistent scoring mechanism to their answers within this framework. Our scoring of the City of Seattle's practices in each of the following domains was based on the AICPA/CICA Privacy Maturity Model (PMM) levels, which reflect Generally Accepted Privacy Principles (GAPP):[1]

- ***Undeveloped*** – procedures or processes are absent, or are unpredictable and reactive.
- ***Ad hoc*** – procedures or processes are generally informal, incomplete, and inconsistently applied.
- ***Repeatable*** – procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
- ***Defined*** – procedures and processes are fully documented and implemented, and cover all relevant aspects.
- ***Managed*** – reviews are conducted to assess the effectiveness of the controls in place.
- ***Optimized*** – regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

[1] *See* AICPA/CICA PRIVACY TASK FORCE, AICPA/CICA PRIVACY MATURITY MODEL, (2011), https://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf

A key principle of the PMM approach is the recognition that "each organization's personal information privacy practices may be at various levels, whether due to legislative requirements, corporate policies or the status of the organization's privacy initiatives. It was also recognized that based on an organization's approach to risk, not all privacy initiatives would need to reach the highest level on the maturity model."[2]

Privacy leadership and program management

- Does the municipality employ a comprehensive, strategic, agency-wide privacy program regarding its open data initiatives?
- Has the municipality designated a privacy governance leader for open data?
- Is the open data program guided by core privacy principles and policies?
- Does the open data workforce receive effective privacy training and education?
- Are the municipality's open data privacy policies and procedures updated in light of ongoing monitoring and periodic assessments?

Maturity score and supporting rationale:

Benefit-risk assessment

- Does the open data program conduct a benefit-risk assessment to manage privacy risk in each dataset considered for publication?
- Are datasets assessed based on the identifiability, sensitivity, and utility of the data prior to release?
- Are inventories of published personally identifiable information (PII) maintained?
- Are benefit-risk assessments documented and regularly reviewed?
- Does the open data program have a mechanism in place to trigger re-assessment of a published dataset in light of new facts?
- Does the open data program have an ability to elevate review of risky or sensitive datasets to disclosure control experts or a disclosure review board?

Maturity score and supporting rationale:

De-identification tools and strategies

- Does the open data program utilize technical, legal, and administrative safeguards to reduce re-identification risk?

[2] *See id.*

- Does the open data program have access to disclosure control experts to evaluate re-identification risk?
- Does the open data program have access to appropriate tools to de-identify unstructured or dynamic data types? (e.g., geographic, video, audio, free text, real time sensor data)
- Does the open data program have policies and procedures for evaluating re-identification risk across databases? (e.g., risk created by intersection of multiple municipal databases; county, state, or federal open databases; commercial databases)
- Does the open data program evaluate privacy risk in light of relevant public records laws?

Maturity score and supporting rationale:

Data quality

- Does the municipality employ policies and procedures for the open data program to ensure that personally identifiable information is accurate, complete, and current?
- Does the open data program check for, and correct as appropriate, inaccurate or outdated personally identifiable information?
- Are there procedures or mechanisms for individuals to submit correction requests for potentially incorrect personal data posted on the open data program?

Maturity score and supporting rationale:

Equity and fairness

- Were the conditions under which the data was collected fair? (e.g., were citizens aware that the data would be published on the open data portal? Did individuals have an opportunity to opt out of data collection? If data was acquired from a third party, were terms and conditions observed in the collection, use, maintenance, and sharing of the data?)
- Does the open data program assess the representativeness of the data? (e.g. whether underserved or vulnerable populations are appropriately represented in the data, or whether underserved or vulnerable populations' interests are taken into account when determining what data to publish).
- Are any procedures and mechanisms in place for people to submit complaints about the use of data or about the publication process generally, as well as procedures for responding to those complaints?

Maturity score and supporting rationale:

Transparency and public engagement

- Does the open data program engage and educate the public about the benefits of open data?
- Does the open data program engage and educate the public about the privacy risks of open data?
- Does the open data program provide opportunities for public input and feedback about the portal, the data available, and privacy, utility, or other concerns?
- Does the open data program engage with the public when developing of open data privacy protections?
- Does the open data program consider the public interest in determining what datasets to publish?
- Does the open data program communicate with the public about why some datasets may include PII?

Maturity score and supporting rationale:

Overall Open Data Program privacy maturity score:

Maturity score and supporting rationale: